REMARKS/ARGUMENTS

Favorable reconsideration of this application as presently amended and in light of the following discussion is respectfully requested.

Claims 2-6, 8-14, 16-20, and 22-29 are pending; and Claims 6, 20, and 29 are amended by the present amendment.

Claims 6, 20, and 29 are amended to recite "executable service communication code." Support for this feature is found in the specification at least on page 21, lines 6-10. The remaining changes to the claims are cosmetic, correcting minor informalities and removing language which could be interpreted as invoking 35 U.S.C. §112, sixth paragraph. A "thereby clause" is removed from the claims as this language did not further limit the respective claims. Moreover, language was removed from the claims which could be interpreted as requiring human interaction to infringe the claims. Thus, no new matter is added.

The outstanding Official Action rejected Claims 2-6, 8-14, 16-20, and 22-29 under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 6,088,451 to He et al. (hereinafter He) and further in view of U.S. Patent No. 4,817,050 to Komatsu et al. (hereinafter Komatsu); and Claims 10, 11, 14, 24, 25, and 28 were rejected under 35 U.S.C. § 103(a) as unpatentable over He and Komatsu, and further in view of U.S. Patent No. 5,872,847 to Boyle et al. (hereinafter Boyle).

As a preliminary matter, Applicants request acknowledgement and consideration of the Information Disclosure Statement filed on October 10, 2006 in the next communication.

Applicants acknowledge with appreciate the courtesy of an interview conducted on May 1, 2007 between Applicants' representatives and the Examiner. During the interview, Applicants' representatives discussed Applicants' Figure 1 and discussed proposed claim amendments, similar to those presented herein, to patentably distinguish over the applied references. The Examiner indicated that further consideration would be required in view of the claim amendments. Arguments presented during the interview are reiterated below.

Applicants respectfully traverse the rejection of Claim 6 under 35 U.S.C. § 103(a).

Claim 6 is directed to a system on a server computer system having a communications engine, a security services engine, a web server engine, a host engine, and a keysafe. The communications engine is configured to establish a communications link with a client. The security services engine is coupled to the communications engine and configured to the client a plurality of user authentication protocol options, where each user authentication protocol option has a particular level of authentication associated with it. The security services engine authenticates the user according to at least one user authentication protocol and determines user privileges based on the identity of the user and the level of authentication.

The web server engine is configured to present a set of available services based on the user privileges, where at least one of the available services requires additional authentication information to be provided before access to the service is granted, and enable the client to select a particular service from the set of available services. The host engine is coupled to the security services and to the web server and configured to provide to the client ***executable service communication code*** that enables communication with the particular service.

The keysafe is configured to store keys, where each key enables communication between the client and a service selected from the set of available services and includes all additional authentication information required by the selected service for authenticating the user to the selected service. ***The executable service communication code functions to retrieve a key corresponding to the particular service selected form the keysafe upon***

execution of the code. By storing all the authentication information necessary for each service in the keysafe, the present system enables the client to access the available services without storing the service communication code and keys on a device the client is using.[1] Additionally, the present system reduces the complexity and burden for a roaming client to carry and keep track of which keys to use for each service.[2]

He describes a security system for user access to network elements.[3] The security system in He includes a user element (102), such as a user terminal, an authentication server (202), a credentials server (204), a registration database (210), and a plurality of network elements (104).[4]

In operation, He utilizes user identification and registration which requires that each user be assigned a network wide unique identifier and that a database be used for registration and management of the user accounts. The registration database (210) is used to hold the information for the user accounts. A user account shall consist of the unique user identifier as well as other essential user information for the control system to make access decisions for the user.[5]

He describes the following authentication process. First, the user employs a user element (102) and initiates the authentication process by requesting to send a request message to the authentication server (202). The request message contains the user identifier presented to the authentication server (202) for user network authentication.[6] Upon receiving the user request message, an authentication server (202) uses the identifier in the message to look up the user registration database (210) and retrieves a record corresponding to that user (user record). A response message prepared by the authentication server (202) is sent back to the

[1] See specification at page 17, lines 14-21 and original claim 6.
[2] See specification at page 4, line 17 to page 5, line 3.
[3] See He at column 1, lines 55-56.
[4] See He at column 11, lines 54-65 and Figure 2.
[5] See He at column 16, lines 27-37.
[6] See He at column 17, lines 55-60.

user containing a general ticket for the user to communicate with the credential server (204). The message also contains a secret key generated by the authentication server (202) that facilitates secure communications between the user and the credential server (204).[7] Upon receiving the response message, the user will be requested to present the correct secret key to a local access control system in the user element (102). The user supplied secret key is then used to decrypt the response message for the user to retrieve the correct ticket, which allows the user to access the network.[8]

Claim 6 is distinguishable over He as the applied reference fails to disclose or suggest ***providing executable service communication code to the client***. He merely describes that upon a request access a network, the authentication server provides the user with a response message containing a ticket and a secret key, which are used to authenticate the user's access to the network. As known by those ordinarily skilled in the art, ***executable code*** is a set of encoded instructions causing a computer to implement a process. A ticket and a secret key are not ***executable code*** as these two items are merely ***non-executable*** digital information used in an authentication process.

Furthermore, He fails to disclose or suggest ***executable code functioning to retrieve a key corresponding to a selected service from the keysafe upon execution of the code***. The outstanding Official Action identifies the registration database (210) as a keysafe.[9] He merely describes that upon receiving a network access request containing a user identifier, the authentication server retrieves a record from the registration database corresponding to the user identifier. He neither discloses nor suggests that a key is retrieved the registration database (210). Furthermore, the secret key supplied to the user is generated by the authentication server instead of being retrieved from the registration database (210).[10]

[7] See He at column 17, line 61 to column 18, line 7.
[8] See He at column 18, lines 8-26.
[9] See Official Action of November 17, 2006 at page 3, paragraph (i)(5).
[10] See He at column 18, lines 2-3.

As Komatsu is not cited in the Official Action as disclosing the aforementioned features and certainly fails to cure the deficiencies discussed above, Applicants submit that He and Komatsu fail to disclose or suggest all the limitations recited in Claim 6. Therefore, Applicants respectfully request that the rejection of Claim 6, and claims depending therefrom, under 35 U.S.C. § 103(a) be withdrawn.

As independent Claims 20 and 29 are amended to recite features analogous to those recited in Claim 6, Applicants submit that He and Komatsu fail to disclose or suggest all the limitations of Claims 20 and 29. Therefore, Applicants respectfully request that the rejection of Claims 20 and 29, and claims depending therefrom, under 35 U.S.C. § 103(a) be withdrawn.

The Official Action has rejected Claims 10, 11, 14, 24, 25, and 28 under 35 U.S.C. § 103(a) over He and Komatsu, and further in view of Boyle.

As outlined above, He and Komatsu fail to disclose or suggest all the limitations of Claims 6, 20, and 29, which Claims 10, 11, 14, 24, 25, and 28 depend therefrom. As Boyle does not remedy the deficiency discussed above, Applicants submit that a *prima facie* case of obviousness has not been presented.

Accordingly, Applicants respectfully request that the rejection of Claims 10, 11, 14, 24, 25, and 28 under 35 U.S.C. § 103(a) be withdrawn.

Consequently, in view of the present response, no further issues are believed to be outstanding in the present application, and the present application is believed to be in condition for formal allowance. A Notice of Allowance for Claims 2-6, 8-14, 16-20, and 22-29 is earnestly solicited.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Scott A. McKeown
Attorney of Record
Registration No. 42,866

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

I:\ATTY\SP\30'S\303600US\303600US-AM.DOC